1. A method of preventing the repudiation of digitally-signed electronic documents, the method comprising the steps of:

receiving a plurality of electronic documents during a first and second time interval;

forming a message digest for each of the plurality of electronic documents;

forming a first super-message digest derived at least in part from each of the message digests received during the first time interval;

forming a second super-message digest derived at least in part from each of the message digests received during the second time interval and from the first super-message digest;

transmitting the second super-message digest to a timestamp authority and receiving a timestamp therefrom; and

recording each of the message digests, first and second super-message digests, and timestamp in an audit log.

2. The method of claim 1 wherein at least one of the plurality of electronic documents corresponds to a file attachment in an electronic mail message.

3. The method of claim 1 wherein the first and second time intervals are pre-determined.

4. The method of claim 1 wherein the duration of the first and second time intervals are dynamically determined from a number of electronic documents anticipated during a particular time of day.

5. The method of claim 1 further comprising the step of recording a timestamp associated with the first super-message digest in the audit log.

6. The method of claim 5 wherein the first super-message digest is further derived from the timestamp associated with the first super-message digest and from a prior super-message digest.

7. The method of claim 5 wherein the second super-message digest is further derived from the timestamp associated with the first super-message digest.

8. A method of securely delivering an electronic document, the method comprising the steps of:

at a message server associated with a sender of the electronic document,

computing a symmetric key from message parameters associated with the electronic document and from a hidden parameter associated with the message server using a predefined algorithm;

encrypting the electronic document using the symmetric key;

transmitting the encrypted electronic document and the message parameters to at least one recipient;

at a web server coupled to the recipient of the encrypted electronic document,

receiving identification data associated with the recipient;

receiving the message parameters transmitted to the recipient;

comparing the identification data associated with the recipient with the received message parameters;

upon matching the identification data with at least some of the received message parameters, dynamically computing the symmetric key from the received message parameters and the hidden parameter associated with the message server using the predefined algorithm; and

providing the symmetric key to the recipient.

9. The method of claim 8 wherein the electronic document is digitally signed.

10. The method of claim 8 wherein the message parameters include a recipient list and a hash of the electronic document.

11. The method of claim 8 wherein the electronic document and message parameters are transmitted to the recipient in an electronic mail message.

12. The method of claim 11 wherein the received message parameters are posted to the web server via an HTML form included in the electronic mail message.

13. The method of claim 8 wherein the identification data includes a user ID and password previously registered by the web server.

14. The method of claim 8 wherein the message server and the web server are controlled by the sender of the electronic document.

15. A method of securely delivering an electronic document via a web server, the method comprising the steps of:

receiving a symmetrically encrypted electronic document and parameters associated therewith, the parameters including a recipient list associated with the electronic document;

receiving identification data from the recipient via a communications network and comparing at least some of the received parameters therewith;

upon matching the identification data and the at least some of the received parameters, dynamically computing a symmetric key from the received parameters;

decrypting the electronic document using the symmetric key; and

displaying the decrypted document on a web page accessible to the recipient.

16. The method of claim 15 further comprising the step of transmitting a message to a sender of the symmetrically encrypted electronic document after matching the identification data and the received parameters.